Cybersecurity Incident Report:
Website Compromise – Yummyrecipesforme.com

Section 1: Identify the network protocol involved

The protocols observed during the tcpdump capture were:
• **DNS (Domain Name System)** – Used to resolve the IP addresses for yummyrecipesforme.com and later greatrecipesforme.com.
• **HTTP (Hypertext Transfer Protocol)** – Used by the browser to send requests and download content from the web server.

These protocols were abused during the incident to redirect users and deliver malicious files.

Section 2: Document the incident

Incident Summary:
The website yummyrecipesforme.com was compromised following a brute force attack on the administrative account of the web server. The attacker gained access by repeatedly trying default passwords until the correct one was guessed. Once logged in, the attacker altered the website's source code to insert a malicious JavaScript snippet.

Sequence of Events (based on tcpdump logs):
1. The user's browser initiated a DNS request for yummyrecipesforme.com and received the correct IP address.
2. The browser initiated an HTTP request to load the website.
3. The website source code triggered a malicious file download prompt.
4. Once the file was executed, the browser sent another DNS request for greatrecipesforme.com.
5. The browser was redirected and initiated HTTP requests to the fake site, which contained malware.

Impact and Evidence:
• Multiple customers reported being prompted to download a suspicious file when visiting the legitimate site.
• Running the file redirected them to greatrecipesforme.com, which slowed down their personal computers.
• The senior analyst confirmed the website's source code had been modified and contained malicious JavaScript.
• The web server had weak protections in place (default password, no brute force prevention).

How it was discovered:
The incident came to light after multiple customer complaints to the helpdesk. The hosting provider also confirmed that the admin password had been changed, locking out the legitimate owner.

Section 3: Recommend one security measure

Recommendation:
Implement **Two-Factor Authentication (2FA)** for all administrative logins.

Why this is effective:
• Even if an attacker guesses or brute forces the password, they would still need the second factor (e.g., a code sent via an authenticator app or SMS).
• 2FA greatly reduces the effectiveness of brute force attacks and prevents unauthorized access even when weak or default passwords are in use.
• Combined with strong password policies, 2FA adds an essential extra layer of defense for critical admin accounts.